UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,405	08/30/2001	Robert P. Goldman	H0001867 (FSP:114.001US01	8248

7590 05/16/2006

Honeywell International Inc.
Law Dept. AB2
P.O. Box 2245
Morristown, NJ 07962-9806

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/943,405	GOLDMAN ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/6/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Amendment

1. This office action is responsive to Applicant's amendment received on 2/17/2006. Claims 1-20 are pending.

Response to Arguments

2. Applicant's arguments filed 2/17/2006 have been fully considered but they are not persuasive.

Applicant mainly argues that Gleichauf et al., (Gleichauf hereinafter) does not disclose a security goal database that describes uses that hardware and software installed on the network may support.

Examiner respectfully responds that Gleichauf does disclose "a rule-driven, multi-phase network vulnerability assessment process to discover network information such as ***devices, operating systems, and services*** on the internal network 10. ... For example, the embodiment of FIG. 3, network security system 20 can identify the device type 70 of each device or system coupled to internal network 10. Network security system 20 can further identify the operating system 74 of each device and the services 78 available on each device. Additionally, the network security system 20 of FIG. 2 can make an assessment of potential vulnerabilities 80 associated with each device on internal network 10" (i.e., it is inherently disclosed that the rule-driven vulnerability assessment process has to be done through ***comparing*** the discovered information of ***devices, operating systems, and services*** with some pre-defined rule sets)(col. 7, lines 40-65). Such a ***rule set*** is expressly disclosed in U.S. Patent application Ser. No.

09/107,964, entitled "System and Method for Rules-Driven Multi-Phase Network Vulnerability Assessment," which is incorporated by reference in Gleichauf (col. 6, lines 1-5).

Allowable Subject Matter

3. The indicated allowability of claims 19 and 20 are withdrawn in view of a more detailed interpretation of the cited prior art.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Gleichauf et al., (U.S. Patent No. 6,301,668 and Gleichauf hereinafter).

Regarding claims 1 and 13, Gleichauf discloses a network reference model for use in configuring security software on a computer network, the network reference model comprising:

a database engine providing deduction, a network information database associated with the database engine and providing a central repository for a configuration of hardware and software installed on the network (Col. 5, lines 33-67), and a security goal database associated with the database engine and describing uses

that the hardware and software installed on the network may support (Col. 7, lines 20-65).

Regarding claims 2-10, and 13-14, Gleichauf discloses a configuration tool for use in configuring security software packages on a computer network the configuration tool comprising:

a description logic database engine, a network information database associated with the description logic database engine and providing a central repository for a configuration of hardware and software installed on the network (Col. 5, lines 33-67),

a security goal database associated with the description logic database engine and providing security goals describing uses that the hardware and software of the network may support (Col. 7, lines 1-65),

an event database associated with the description logic database engine and containing events related to the network, wherein the events contained in the event database include possible attacks against the network and benign events that could.be confused with the possible attacks (Col. 5, lines 52-67 and Col. 6, lines 1-15),

a first configuration module coupled to the description logic database engine for configuring intrusion blocking security software packages, a second configuration module coupled to the description logic database engine for configuring intrusion detecting security software packages, a system hardening module coupled to the description logic database engine for automating a process of hardening the network (Col. 6, lines 50-67 and Col. 7, lines 1-25) and

an audit configuration module coupled to the description logic database engine for probing the network for vulnerabilities (Col. 4, lines 1-40),

wherein the first configuration module configures the intrusion blocking security software packages based on the configuration of the hardware and software installed on the network and the security goals, wherein the second configuration module configures the intrusion detecting seculity software packages based on the configuration of the hardware and software installed on the network and the security goals (Col. 7, lines 65-67 and Col. 8, lines 1-67 and Col. 9, lines 1-18), and

wherein the system hardening module is context sensitive (Col. 6, lines 15-45).

Regarding claims 11 and 15, Gleichauf discloses a method for configuring a security software package installed on an individual network device, the method comprising:

using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device, wherein the individual network device is a member of the class of network devices (Col. 5, lines 1-50), and

configuring the security software package using the one or more security goals, wherein the security software package is selected from the group consisting of an intrusion blocking software package and an intrusion detecting software package (Col. 9, lines 4-16).

Regarding claims 12 and 16, Gleichauf discloses wherein using active inference further comprises automatically classifying the individual network device based on an IP address, a network topology and one or more services the individual network device provides, and applying rules to the individual network device based on its classification (Col. 4, lines 40-67 and Col. 6, lines 14-35).

Regarding claims 17 and 18, Gleichauf discloses a method for configuring a security software package, the method comprising:

defining one or more security policies for a class of network devices, wherein the security software package is a service running on at least one network device of the class of network devices (Col. 6, lines 14-35), using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals, using a database engine providing deduction to associate the one or more security goals with the at least one network device (Col. 5, lines 32-67 and Col. 6, lines 1-67), and configuring the security software package on the at least one network device using the one or more security goals (Col. 7, lines 1-25).

Regarding claim 19, Gleichauf dicloses the method of claim 18 wherein generating a second database containing first security goals further comprises generating a second database containing first security goals (i.e., network map) for each class of hardware devices (i.e., scan engine can ping devices, which is done based on the device's IP address, use port scans, rule-driven, and ... to make an

assessment of potencial vulnerabilities associated with each device based on the network map. Concequently, the security system is able to configure and reconfigure itself as the network dynamics dictate)(Fig. 3 and its corresponding text and col. 5, lines 52-67 and col. 6, lines 1-24).

Regarding claim 20, Gleichauf discloses the method of claim 19 wherein decomposing the first security goals for individual hardware devices further comprises using inference to associate the second security goals with individual hardware devices within each class of hardware devices (i.e., analyzing the collected information in the network map to identify potential vulnerabilities)(Fig. 3 and its corresponding text and col. 5, lines 52-67 and col. 6, lines 1-67 and col. 7, lines 1-25).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gleichauf et al., (U.S. Patent No. 6,324,656), and

Vaidya, (U.S. Patent No. 6,279,113).

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A.S.

Patent Examiner
Group 2131
May 10, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100